IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA

HEATHER MCCREEDY, SCOTT GIBSON, KATHRYN ROHRER, LATOYA LINDSEY, MICHAEL SMELLEY, ROBERT DURHAM, STACY LOWE, STEPHANIE JENNINGS, TIRANCE KENNEDY, BRIAN JAMES, BROOKE PENNINGTON, CHARLES LEE CARLISLE, CONNIE MONTALVO, DON SHILLING, DAVID TURBEN, DANA JONES, JOSE GARCIA, JOSEPH DODSON, HOWARD R. HERSHIPS, JOHN R. WILKINSON III, JAMILA HUNTER, and ERIC SPEACH individually and on behalf of all others similarly situated,

Plaintiffs,

v.

PURPOSE FINANCIAL, INC. f/k/a ADVANCE AMERICA CASH ADVANCE CENTERS, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF TENNESSEE, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF CALIFORNIA, LLC, ADVANCE AMERICA, CASH ADVANCE CENTERS OF MISSISSIPPI, LLC, ADVANCE AMERICA, CASH ADVANCE CENTERS OF FLORIDA, LLC, ADVANCE AMERICA, CASH ADVANCE CENTERS OF OHIO, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF NEVADA, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF MICHIGAN, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF KENTUCKY, INC., and ADVANCE AMERICA, CASH ADVANCE CENTERS OF INDIANA, INC.

Defendants.

C/A No. 7:23-cv-04256-DCC

CONSOLIDATED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs, Heather McCreedy, Scott Gibson, Larry Musgrave, Kathryn Rohrer, LaToya Lindsey, Michael Smelley, Robert Durham, Stacy Lowe, Stephanie Jennings, Tirance Kennedy, Brian James, Brooke Pennington, Charles Lee Carlisle, Connie Montalvo, Don Shilling, David Turben, Dana Jones, Jose Garcia, Joseph Dodson, Howard R. Herships, John R. Wilkinson III, Jamila Hunter, and Eric Speach ("Plaintiffs") bring this Consolidated Class Action Complaint, individually and on behalf of all others similarly situated, and by and through their undersigned counsel, against Defendants Purpose Financial, Inc. f/k/a Advance America Cash Advance Centers, Inc., Advance America, Cash Advance Centers of Tennessee, Inc., Advance America, Cash Advance Centers of California, LLC, Advance America, Cash Advance Centers of Mississippi, LLC, Advance America, Cash Advance Centers of Florida, LLC, Advance America, Cash Advance Centers of Ohio, Inc., Advance America, Cash Advance Centers of Nevada, Inc., Advance America, Cash Advance Centers of Michigan, Inc., Advance America, Cash Advance Centers of Kentucky, Inc. and Advance America, Cash Advance Centers of Indiana, Inc. (collectively, "Defendants" or "Advance America") and allege the following, based upon personal knowledge with respect to themselves, and, upon information and belief, based on the investigation of their counsel as to all other matters.

NATURE OF THE ACTION

1. This class action arises out of the recent preventable cyberattack and data breach resulting from Advance America's negligent failure to implement reasonable and industry standard data security practices.

2. Through a nationwide network of subsidiaries and online, Advance America provides high rate financing services direct to consumers including payday loans, installment loans, lines of credit and cash advance services.

3. To provide these services and in the ordinary course of Advance America's business, Advance America requires its customers to provide their personally identifiable information ("PII"), including, but not limited to: their names and Social Security numbers.

4. Advance America operates a shared IT network, on which it stores the sensitive PII of Plaintiffs and Class Members in an unencrypted manner and in an internet accessible environment. On or about February 7, 2023, cybercriminals accessed Advance America's inadequately secured network, containing the PII of Plaintiffs and Class Members (the "Data Breach"), and were able to "access[] or acquire[] certain corporate business records on [Advanced America's] network."[1]

5. Advance America was negligent in its cybersecurity architecture and inadequately protected its customers' PII.

6. Although the Social Security numbers of Plaintiffs and Class Members had been acquired in the Data Breach, Advance America inexplicably waited approximately six (6) months, until August 2023, to begin notifying victims of the Data Breach.

7. Advance America's misconduct—being negligent and/or reckless by failing to implement adequate and reasonable data security measures to protect Plaintiffs' and Class Members' PII, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that they did not have adequate security practices and employee training in place to safeguard the PII, failing to honor their promises and representations to protect Plaintiffs' and Class Members' PII, and failing to provide

[1] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/ad6aff52-874f-4461-b98b-1e7cba93d6ea.shtml (last accessed Nov. 21, 2023).

timely and adequate notice of the Data Breach— caused substantial harm and injuries to Plaintiffs and Class Members across the United States.

8. The Data Breach was a direct result of Defendants' conduct and failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect their customers' PII from a foreseeable and preventable cyber-attack.

9. Defendants maintained the PII in a reckless and negligent manner. The PII was maintained on Defendants' computer network(s) in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

10. Defendants disregarded the rights of Plaintiffs and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

11. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct because the PII that Defendants collected and maintained is now in the hands of data thieves.

12. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new fraudulent financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax

returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest. This risk will continue for the rest of their lives, as Plaintiffs and Class Members are now forced to deal with the danger of identity thieves possessing and fraudulently using their PII.

13. Plaintiffs bring this Class Action on behalf all those similarly situated to address Defendants' negligence and inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

14. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

15. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

THE PARTIES

Plaintiffs

16. Plaintiff Heather McCreedy is a citizen and resident of the state of Florida.

17. Plaintiff Scott Gibson is a citizen and resident of the state of California.

18. Plaintiff Kathryn Rohrer is a citizen and resident of the state of California.

19. Plaintiff LaToya Lindsey is a citizen and resident of the state of Michigan.

20. Plaintiff Michael Smelley is a citizen and resident of the state of Nevada.

21. Plaintiff Robert Durham is a citizen and resident of the state of Ohio.

22. Plaintiff Stacy Lowe is a citizen and resident of the state of Florida.

23. Plaintiff Stephanie Jennings is a citizen and resident of the state of Tennessee.

24. Plaintiff Tirance Kennedy is a citizen and resident of the state of Mississippi.

25. Plaintiff Brian James is a citizen and resident of the state of Indiana.

26. Plaintiff Brooke Pennington is a citizen and resident of the state of Kentucky.

27. Plaintiff Charles Lee Carlisle is a citizen and resident of the state of Florida.

28. Plaintiff Connie Montalvo is a citizen and resident of the state of Florida.

29. Plaintiff Don Shilling is a citizen and resident of the state of Florida.

30. Plaintiff David Turben is a citizen and resident of the state of Ohio.

31. Plaintiff Dana Jones is a citizen and resident of the state of Tennessee.

32. Plaintiff Jose Garcia is a citizen and resident of the state of California.

33. Plaintiff Joseph Dodson is a citizen and resident of the state of Ohio.

34. Plaintiff Howard R. Herships is a citizen and resident of the state of California.

35. Plaintiff John R. Wilkinson III is a citizen and resident of the state of Tennessee.

36. Plaintiff Jamila Hunter is a citizen and resident of the state of Florida.

37. Plaintiff Eric Speach is a citizen and resident of the state of Tennessee.

Defendants

38. Defendant Purpose Financial Inc. f/k/a Advance America Cash Advance Centers, Inc. is a Delaware corporation with its principal place of business in South Carolina. Purpose Financial, Inc. is a subsidiary of Eagle U.S. Sub, Inc. Eagle U.S. Sub, Inc. is a subsidiary of Grupo Elektra, S.A.B. de C.V. Grupo Elektra, S.A.B. de C.V. is publicly traded on the Bolsa Mexicana de Valores (the Mexican Stock Exchange).

39. Purpose Financial, Inc. is the parent company of a nationwide network of subsidiary companies (listed below) which each operate in and serve consumers in their respective states. Purpose Financial, Inc. directs and controls each of its subsidiaries, all of whom share an IT

network on which the PII of Class Members was stored and/or from which it was accessible. Moreover, on information and belief, each of Purpose Financial Inc.'s subsidiaries were directed and operated from a common corporate headquarters in Spartanburg, South Carolina and through common corporate personnel.

40. Defendant Advance America, Cash Advance Centers of Tennessee, Inc. is a Delaware corporation with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Tennessee, Inc. d/b/a Advance America is a subsidiary of Purpose Financial Inc. and serves customers in the state of Tennessee.

41. Defendant Advance America, Cash Advance Centers of California, LLC is a limited liability company formed in Delaware with its principal place of business in Spartanburg, South Carolina. Advance America, Cash Advance Centers of California, LLC d/b/a Advance America is a subsidiary of Purpose Financial Inc. and serves customers in the state of California.

42. Defendant Advance America, Cash Advance Centers of Mississippi, LLC is a Delaware limited liability company with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Mississippi, LLC is a subsidiary of Purpose Financial Inc. and serves customers in the state of Mississippi.

43. Defendant Advance America, Cash Advance Centers of Florida, LLC is a Delaware limited liability company with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Florida, LLC is a subsidiary of Purpose Financial Inc. and serves customers in the state of Florida.

44. Defendant Advance America, Cash Advance Centers of Ohio, Inc. is a Delaware corporation with its principal place of business in South Carolina. Advance America, Cash

Advance Centers of Ohio, Inc. is a subsidiary of Purpose Financial Inc. and serves customers in the state of Ohio.

45. Defendant Advance America, Cash Advance Centers of Nevada, Inc. is a Delaware corporation with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Nevada, Inc. is a subsidiary of Purpose Financial Inc. and serves customers in the state of Nevada.

46. Defendant Advance America, Cash Advance Centers of Michigan, Inc. is a Delaware corporation with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Michigan, Inc. is a subsidiary of Purpose Financial Inc. and serves customers in the state of Michigan.

47. Defendant Advance America, Cash Advance Centers of Kentucky, Inc. is a Delaware corporation with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Kentucky, Inc. is a subsidiary of Purpose Financial Inc. and serves customers in the state of Kentucky.

48. Defendant Advance America, Cash Advance Centers of Indiana, Inc. is a Delaware corporation with its principal place of business in South Carolina. Advance America, Cash Advance Centers of Indiana, Inc. is a subsidiary of Purpose Financial Inc. and serves customers in the state of Indiana.

49. Each of the Defendants are responsible for the unlawful practices and policies alleged herein.

JURISDICTION AND VENUE

50. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100

class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the Class are citizens of states that differ from Defendants.

51. This Court has personal jurisdiction over Defendants because Defendants' principal places of business are in this District and Defendants conduct substantial business in South Carolina and this District through their headquarters and offices.

52. Venue is likewise proper as to Defendants in this District under 28 U.S.C. § 1391 because Defendants are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

53. Advance America operates as a network of subsidiaries which serve consumers of their respective states, each of which are overseen and directed by Purpose Financial.

54. To provide its high-interest rate lending services to consumers, Advance America collects, through its subsidiary companies and affiliates, and centralizes the PII of consumers who solicit or secure lending services on a shared computer network and subject to common data security policies and procedures.

55. Due to the highly sensitive and personal nature of the information Advance America acquires and stores with respect to loan applicants and customers, Advance America recognizes the privacy rights of those individuals, as evidenced by Advance America's publicly available privacy policy ("Privacy Notice")[2], which promises consumers that:

[2] https://cdn.advanceamerica.net/public/media/documents/2022-04/Advance%20America%20Privacy%20Policy.pdf?VersionId=EJZFor.2fa4pWqL.VQo3y5rP_Q1oqQte&_ga=2.117377798.1684359604.1692898536-294395171.1692750439.

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.

56. Defendants' Security Information, posted on their website, states as follows:

> **Security of Your Information with Advance America**
>
> With Advance America, you can be sure that all the information you submit is sent through a secure server, and we keep your information in a secure database.

57. Defendants' website also states "[a]ll of our online loan applications include robust security and encryption to ensure your personal data is as secure as possible."

58. Based on these promises, Plaintiffs and the Class Members reasonably expected that Advance America would implement and maintain reasonable data security measures to protect their PII from the foreseeable threat of a data breach.

59. Plaintiffs and Class Members provided their PII to Advance America with the reasonable expectation and on the mutual understanding that Advance America would comply with its obligations to keep such information confidential and secure from unauthorized access.

60. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Advance America to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

61. Advance America had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Advance America has a legal duty to keep consumer's PII safe and confidential.

62. Advance America had obligations created by FTC Act, Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

63. Advance America derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Advance America could not perform the services they provide.

64. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Advance America assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

65. On or around March 23, 2023, reports began surfacing on the Internet that Defendants had been the subject of a ransomware attack by the "BlackBasta" ransomware family and that information obtained during the attack had surfaced on the dark web, including samples containing Social Security numbers and driver's license numbers.

66. In August 2023, Advance America and its subsidiaries began sending Plaintiffs and other Data Breach victims a Notice of Data Breach letter (the "Notice Letter"), informing them that:

> **What Happened**
>
> On or around February 7, 2023, we experienced a temporary systems outage affecting our corporate network. Upon becoming aware of the incident, we immediately launched an investigation to better understand the scope and impact of the incident. We also engaged third-party cybersecurity experts to remediate, further investigate what happened, and determine the scope of the incident. Our investigation determined that an unauthorized actor accessed or acquired certain corporate business records on the Company's network. We also reported this incident to law enforcement.
>
> **What We Discovered**

> We conducted a thorough review of these business records to identify the individuals whose information was contained in the records. We recently completed this review and determined that some of your information was included in the records.
>
> **What Information Was Involved**
> The impacted personal information relating to you includes your Social Security number.[3]

67. Omitted from the Notice Letter were the dates of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

68. The notices that Defendants sent to various states Attorneys General and to Plaintiffs and Class Members did not disclose that (i) Plaintiffs' and Class Members' PII was actually acquired by an unauthorized actor during the Data Breach, (ii) the PII had been made available for sale on the dark web, and (iii) whether the threat actor had demanded a ransom and, if so, whether Defendants has refused to pay it.

69. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

70. Advance America did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class

[3] The Notice Letter.

Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

71. The attacker accessed and acquired files Advance America shared with a third party containing unencrypted PII of Plaintiffs and Class Members, including their Social Security numbers and other sensitive information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

72. As numerous Plaintiffs have already experienced, the PII of Class Members was or will be subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

B. Plaintiffs' Experiences

Plaintiff Heather McCreedy

73. Plaintiff McCreedy is a former customer at Advance America, Cash Advance Centers of Florida, LLC.

74. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

75. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff McCreedy's PII in its system, including her name, Social Security number, and other sensitive information.

76. Plaintiff McCreedy is very careful about sharing her sensitive PII. Plaintiff McCreedy stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

77. Plaintiff McCreedy received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

78. Upon information and belief, Plaintiff McCreedy's PII has not been compromised in a prior Data Breach.

79. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff McCreedy made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff McCreedy has spent significant time dealing with the Data Breach, valuable time Plaintiff McCreedy otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

80. Plaintiff McCreedy suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

81. Plaintiff McCreedy also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

82. The Data Breach has caused Plaintiff McCreedy to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

83. As a result of the Data Breach, Plaintiff McCreedy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff McCreedy is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Scott Gibson

84. Plaintiff Gibson is a former customer at Advance America, Cash Advance Centers of California, LLC.

85. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

86. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Gibson's PII in its system, including his name, Social Security number, and other sensitive information.

87. Plaintiff Gibson is careful about sharing his sensitive PII. Plaintiff Gibson stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

88. Plaintiff Gibson received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

89. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Gibson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to reviewing his various financial and credit account. Plaintiff Gibson has spent significant time dealing with the Data Breach, valuable time Plaintiff Gibson otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

90. Plaintiff Gibson suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

91. Plaintiff Gibson also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

92. The Data Breach has caused Plaintiff Gibson to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed his of key details about the Data Breach's occurrence.

93. As a result of the Data Breach, Plaintiff Gibson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Gibson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Kathryn Rohrer

94. Plaintiff Rohrer is a former customer at Advance America, Cash Advance Centers of California, LLC.

95. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

96. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Rohrer's PII in its system, including her name, Social Security number, and other sensitive information.

97. Plaintiff Rohrer is very careful about sharing her sensitive PII. Plaintiff Rohrer stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

98. Plaintiff Rohrer received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

99. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Rohrer made reasonable efforts to mitigate the impact of the Data Breach,

including but not limited to replacing impacted credit cards and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Rohrer has spent significant time dealing with the Data Breach, valuable time Plaintiff Rohrer otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

100. Plaintiff Rohrer suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

101. Plaintiff Rohrer additionally suffered actual injury in the form of experiencing unauthorized charges to her Amazon account, which, upon information and belief, was caused by the Data Breach. Moreover, Plaintiff Rohrer paid out-of-pocket costs to replace the impacted credit card.

102. Plaintiff Rohrer further suffered actual injury in the form of her credit score being damaged, resulting in a worse rate for a car loan that she received, which, upon information and belief, was caused by the Data Breach.

103. Plaintiff Rohrer also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

104. The Data Breach has caused Plaintiff Rohrer to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

105. As a result of the Data Breach, Plaintiff Rohrer anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rohrer is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff LaToya Lindsey

106. Plaintiff Lindsey is a former customer at Advance America, Cash Advance Centers of Michigan, Inc.

107. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

108. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Lindsey's PII in its system, including her name, Social Security number, and other sensitive information.

109. Plaintiff Lindsey is very careful about sharing her sensitive PII. Plaintiff Lindsey stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

110. Plaintiff Lindsey received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

111. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Lindsey made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: contacting banks to sort of fraudulent activity on her accounts, contacting banks to place fraud alerts on her accounts, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Lindsey has spent significant time dealing with the Data Breach, valuable time Plaintiff Lindsey otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

112. Plaintiff Lindsey suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

113. Plaintiff Lindsey additionally suffered actual injury in the form of experiencing a fraudulent application to open a Chase Bank account falsely under her name, in or about September 2023, which, upon information and belief, was caused by the Data Breach.

114. Plaintiff Lindsey further suffered actual injury in the form of her PII being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

115. Plaintiff Lindsey also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

116. The Data Breach has caused Plaintiff Lindsey to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

117. As a result of the Data Breach, Plaintiff Lindsey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Lindsey is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Michael Smelley

118. Plaintiff Smelley is a former customer at Advance America, Cash Advance Centers of Nevada, Inc.

119. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

120. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Smelley's PII in its system, including his name, Social Security number, and other sensitive information.

121. Plaintiff Smelley is very careful about sharing his sensitive PII. Plaintiff Smelley stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

122. Plaintiff Smelley received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

123. Upon information and belief, Plaintiff Smelley's PII has not been compromised in a prior Data Breach.

124. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Smelley made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Smelley has spent significant time dealing with the Data Breach, valuable time Plaintiff Smelley otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

125. Plaintiff Smelley suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is

subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

126. Plaintiff Smelley further suffered actual injury in the form of credit cards being fraudulently opened under his name, which, upon information and belief, was caused by the Data Breach.

127. Plaintiff Smelley also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

128. The Data Breach has caused Plaintiff Smelley to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence. Moreover, due to his increased anxiety and stress as a result of the Data Breach, Plaintiff sought medical care and was prescribed an additional blood pressure medication by his provider.

129. As a result of the Data Breach, Plaintiff Smelley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Smelley is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

130. Plaintiff Smelley has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Robert Durham

131. Plaintiff Durham is a current customer at Advance America, Cash Advance Centers of Ohio, Inc.

132. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

133. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Durham's PII in its system, including his name, Social Security number, and other sensitive information.

134. Plaintiff Durham is very careful about sharing his sensitive PII. Plaintiff Durham stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

135. Plaintiff Durham received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

136. Upon information and belief, Plaintiff Durham's PII has not been compromised in a prior Data Breach.

137. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Durham made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Durham has spent significant time dealing with the Data Breach, valuable time Plaintiff Durham otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

138. Plaintiff Durham suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

139. Plaintiff Durham further suffered actual injury in the form of an identity thief using his PII to file a fraudulent dispute on tax payments that Plaintiff previously paid, which Chase Bank subsequently released money for into Plaintiff's checking account, which, upon information and belief, was caused by the Data Breach.

140. Plaintiff Durham additionally suffered actual injury in the form of an identity thief cashing unauthorized checks under his name, which resulted in funds being taken out of Plaintiff's Chase Bank account and Chase Bank closing Plaintiff's account, which, upon information and belief, was caused by the Data Breach. Moreover, Plaintiff currently owes Chase Bank $3,000 as a result of this fraudulent activity, and Plaintiff has been forced to borrow money and sell his personal belongings in order to make bill payments to Chase Bank.

141. Plaintiff Durham also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. Specifically, Plaintiff has experienced phishing attempts from a person impersonating Advance America so as to induce Plaintiff into providing them with additional personal information, which, upon information and belief, would be used to defraud Plaintiff.

142. The Data Breach has caused Plaintiff Durham to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence. Moreover, Plaintiff has been prescribed a medication by his provider to treat his increased stress and anxiety resulting from the Data Breach.

143. As a result of the Data Breach, Plaintiff Durham anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Durham is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

144. Plaintiff Durham has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Stacy Lowe

145. Plaintiff Lowe signed up for services from Advance America, Cash Advance Centers of Florida, LLC, although she never obtained services from Advance America.

146. In order to sign up to apply for services at Advance America, she was required to provide her sensitive PII to Advance America.

147. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Lowe's PII in its system, including her name, Social Security number, and other sensitive information.

148. Plaintiff Lowe is very careful about sharing her sensitive PII. Plaintiff Lowe stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

149. Plaintiff Lowe received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

150. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Lowe made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: replacing impacted debit cards and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Lowe has spent significant time dealing with the Data Breach, valuable time Plaintiff Lowe otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

151. Plaintiff Lowe suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

152. Plaintiff Lowe further suffered actual injury in the form of experiencing fraudulent charges to her debit card, in or about October 2023, which, upon information and belief, was caused by the Data Breach.

153. Plaintiff Lowe further suffered actual injury in the form of her credit score being damaged, which, upon information and belief, was caused by the Data Breach.

154. Plaintiff Lowe also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

155. The Data Breach has caused Plaintiff Lowe to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

156. As a result of the Data Breach, Plaintiff Lowe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Lowe is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Stephanie Jennings

157. Plaintiff Jennings is a former customer at Advance America, Cash Advance Centers of Tennessee, Inc.

158. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

159. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Jennings' PII in its system, including her name, Social Security number, and other sensitive information.

160. Plaintiff Jennings is very careful about sharing her sensitive PII. Plaintiff Jennings stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

161. Plaintiff Jennings received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

162. Upon information and belief, Plaintiff Jennings' PII has not been compromised in a prior Data Breach.

163. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Jennings made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: replacing impacted debit cards and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Jennings has spent significant time dealing with the Data Breach, valuable time Plaintiff Jennings otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

164. Plaintiff Jennings suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

165. Plaintiff Jennings further suffered actual injury in the form of fraudulent charges to her debit card, which, upon information and belief, was caused by the Data Breach.

166. Plaintiff Jennings also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

167. The Data Breach has caused Plaintiff Jennings to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

168. As a result of the Data Breach, Plaintiff Jennings anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Jennings is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Tirance Kennedy

169. Plaintiff Kennedy is a former customer at Advance America, Cash Advance Centers of Mississippi, LLC.

170. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

171. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Kennedy's PII in its system, including his name, Social Security number, and other sensitive information.

172. Plaintiff Kennedy is very careful about sharing his sensitive PII. Plaintiff Kennedy stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

173. Plaintiff Kennedy received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

174. Upon information and belief, Plaintiff Kennedy's PII has not been compromised in a prior Data Breach.

175. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Kennedy made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Kennedy has spent significant time dealing with the Data Breach, valuable time Plaintiff Kennedy otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

176. Plaintiff Kennedy suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

177. Plaintiff Kennedy further suffered actual injury in the form of his PII being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

178. Plaintiff Kennedy also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

179. The Data Breach has caused Plaintiff Kennedy to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

180. As a result of the Data Breach, Plaintiff Kennedy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Kennedy is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Brian James

181. Upon information and belief, Plaintiff James is a former customer at Cash Advance Centers of Indiana, Inc.

182. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

183. At the time of the Data Breach—on or around February 7, 2023—Advance America retained Plaintiff James' PII in its system, including his name, Social Security number, and other sensitive information.

184. Plaintiff James is very careful about sharing his sensitive PII. Plaintiff James stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

185. Plaintiff James received the Notice Letter, by U.S. mail, directly from Advance America, dated August 15, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including their Social Security number.

186. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff James made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his accounts for fraudulent activity, which may take years to detect. Plaintiff James has spent significant time dealing with the Data Breach, valuable time Plaintiff James otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

187. Plaintiff James suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

188. Plaintiff James further suffered actual injury in the form of his PII being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

189. Plaintiff James also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

190. The Data Breach has caused Plaintiff James to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

191. As a result of the Data Breach, Plaintiff James anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff James is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

192. Plaintiff James has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Brooke Pennington

193. Plaintiff Pennington is a former customer at Advance America, Cash Advance Centers of Kentucky, Inc.

194. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

195. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Pennington's PII in its system, including her name, Social Security number, and other sensitive information.

196. Plaintiff Pennington is very careful about sharing her sensitive PII. Plaintiff Pennington stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

197. Plaintiff Pennington received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

198. Upon information and belief, Plaintiff Pennington's PII has not been compromised in a prior Data Breach.

199. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Pennington made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Pennington has spent significant time dealing with the Data Breach, valuable time Plaintiff Pennington otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

200. Plaintiff Pennington suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is

subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

201. Plaintiff Pennington also suffered actual injury in the form of experiencing identity theft in or about the summer of 2023, which, upon information and belief, was caused by the Data Breach.

202. Plaintiff Pennington also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. Specifically, Plaintiff has received spam/phishing attempt calls from parties, including from someone purporting to inquire about a debt consolidation loan that Plaintiff did not apply for.

203. The Data Breach has caused Plaintiff Pennington to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence. Moreover, due to the increased anxiety and stress Plaintiff is experiencing as a result of the Data Breach, Plaintiff sought medical care from her provider and was prescribed anxiety medications.

204. As a result of the Data Breach, Plaintiff Pennington anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Pennington is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Charles Lee Carlisle

205. Plaintiff Carlisle is a former customer at Advance America, Cash Advance Centers of Florida, LLC.

206. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

207. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Carlisle's PII in its system, including his name, Social Security number, and other sensitive information.

208. Plaintiff Carlisle is very careful about sharing his sensitive PII. Plaintiff Carlisle stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

209. Plaintiff Carlisle received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

210. Upon information and belief, Plaintiff Carlisle's PII has not been compromised in a prior Data Breach.

211. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Carlisle made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Carlisle has spent significant time dealing with the Data Breach, valuable time Plaintiff Carlisle otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

212. Plaintiff Carlisle suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

213. Plaintiff Carlisle additionally suffered actual injury in the form of experiencing a fraudulent application for unemployment benefits being submitted under his name, which, upon information and belief, was caused by the Data Breach.

214. Plaintiff Carlisle further suffered actual injury in the form of his credit score being damaged as well as hard inquires being placed on his credit accounts, which, upon information and belief, was caused by the Data Breach.

215. Plaintiff Carlisle also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

216. The Data Breach has caused Plaintiff Carlisle to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

217. As a result of the Data Breach, Plaintiff Carlisle anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Carlisle is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

218. Plaintiff Carlisle has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Connie Montalvo

219. Plaintiff Montalvo is a current customer at Advance America, Cash Advance Centers of Florida, LLC.

220. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

221. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Montalvo's PII in its system, including her name, Social Security number, and other sensitive information.

222. Plaintiff Montalvo is very careful about sharing her sensitive PII. Plaintiff Montalvo stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

223. Plaintiff Montalvo received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

224. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Montalvo made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: reviewing her Experian account for any indication of fraudulent activity, contacting banks to report the fraudulent use of her PII, purchasing a membership to reduce the increase in spam calls, texts, and/or emails that she has experienced, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect.

Plaintiff Montalvo has spent significant time dealing with the Data Breach, valuable time Plaintiff Montalvo otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

225. Plaintiff Montalvo suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

226. Plaintiff Montalvo additionally suffered actual injury in the form of experiencing a fraudulent application for a car loan being submitted under her name, in or about March 2023, which, upon information and belief, was caused by the Data Breach.

227. Plaintiff Montalvo also suffered actual injury in the form of experiencing a fraudulent application for a credit card being submitted under her name, in or about June 2023, which, upon information and belief, was caused by the Data Breach.

228. Plaintiff Montalvo further suffered actual injury in the form of her PII being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

229. Moreover, Plaintiff Montalvo suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the

Data Breach. Moreover, Plaintiff suffered actual injury in the form of paying out-of-pocket costs on a 411 membership to reduce the number of spam calls she receives.

230. The Data Breach has caused Plaintiff Montalvo to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

231. As a result of the Data Breach, Plaintiff Montalvo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Montalvo is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Don Shilling

232. Plaintiff Shilling is a former customer at Advance America, Cash Advance Centers of Florida, LLC.

233. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

234. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Shilling's PII in its system, including his name, Social Security number, and other sensitive information.

235. Plaintiff Shilling is very careful about sharing his sensitive PII. Plaintiff Shilling stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

236. Plaintiff Shilling received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

237. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Shilling made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Shilling has spent significant time dealing with the Data Breach, valuable time Plaintiff Shilling otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

238. Plaintiff Shilling suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

239. Plaintiff Shilling additionally suffered actual injury in the form of a malicious party obtaining his personal information, which, upon information and belief, was caused by the Data Breach.

240. Plaintiff Shilling further suffered actual injury in the form of his PII being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

241. Plaintiff Shilling also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

242. The Data Breach has caused Plaintiff Shilling to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

243. As a result of the Data Breach, Plaintiff Shilling anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Shilling is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

244. Plaintiff Shilling has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff David Turben

245. Upon information and belief, Plaintiff Turben is a former customer at Advance America, Cash Advance Centers of Ohio, Inc.

246. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

247. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Turben's PII in its system, including his name, Social Security number, and other sensitive information.

248. Plaintiff Turben is very careful about sharing his sensitive PII. Plaintiff Turben stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

249. Plaintiff Turben received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

250. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Turben made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: resetting his banking information and otherwise securing his financial accounts, contacting financial institutions to sort out fraudulent activity on his account, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Turben has spent significant time dealing with the Data Breach, valuable time Plaintiff Turben otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

251. Plaintiff Turben suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

252. Plaintiff Turben further suffered actual injury in the form of experiencing fraudulent charges to his Varo Bank account, which, upon information and belief, was caused by the Data Breach.

253. Plaintiff Turben also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

254. The Data Breach has caused Plaintiff Turben to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

255. As a result of the Data Breach, Plaintiff Turben anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Turben is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

256. Plaintiff Turben has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Dana Jones

257. Plaintiff Jones is a current customer at Advance America, Cash Advance Centers of Tennessee, Inc.

258. In order to obtain products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

259. At the time of the Data Breach—on or around February 7, 2023—Advance America retained Plaintiff Jones's PII in its system, including her name, Social Security number, and other sensitive information.

260. Plaintiff Jones is very careful about sharing her sensitive PII. Plaintiff Jones stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

261. Plaintiff Jones received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

262. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Jones made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: signing up for the credit monitoring and identity theft services offered by Advance America, replacing impacted debit cards, contacting financial institutions and credit bureaus to extend fraud alerts and ensure her accounts are secure, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Jones has spent significant time dealing with the Data Breach, valuable time Plaintiff Jones otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

263. Plaintiff Jones suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

264. Plaintiff Jones additionally suffered actual injury in the form of experiencing a fraudulent application for an Amazon credit card being submitted under her name, in or about August 2023, which, upon information and belief, was caused by the Data Breach.

265. Plaintiff Jones also suffered actual injury in the form of an identity thief attempting to use her information for fraudulent activity at KSB Bank, in or about October 2023, which, upon information and belief, was caused by the Data Breach.

266. Plaintiff Jones further suffered actual injury in the form of her PII being disseminated on the dark web, according to Capital One and Experian, which, upon information and belief, was caused by the Data Breach.

267. Plaintiff Jones also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

268. The Data Breach has caused Plaintiff Jones to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence. Moreover, due to the increase anxiety and stress Plaintiff is experiencing as a result of the Data Breach, Plaintiff sought medical care from her provider and had her dosage of medication increased.

269. As a result of the Data Breach, Plaintiff Jones anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Jones is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Jose Garcia

270. Plaintiff Garcia is a former customer at Advance America, Cash Advance Centers of California, LLC.

271. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

272. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Garcia's PII in its system, including his name, Social Security number, and other sensitive information.

273. Plaintiff Garcia is very careful about sharing his sensitive PII. Plaintiff Garcia stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

274. Plaintiff Garcia received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

275. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Garcia made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: signing up for the credit and identity theft monitoring services offered by Advance America and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Garcia has spent significant time dealing with

the Data Breach, valuable time Plaintiff Garcia otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

276. Plaintiff Garcia suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

277. The Data Breach has caused Plaintiff Garcia to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

278. As a result of the Data Breach, Plaintiff Garcia anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Garcia is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

279. Plaintiff Garcia has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Joseph Dodson

280. Plaintiff Dodson is a former customer at Advance America, Cash Advance Centers of Ohio, Inc.

281. In order to obtain products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

282. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Dodson's PII in its system, including his name, Social Security number, and other sensitive information.

283. Plaintiff Dodson is very careful about sharing his sensitive PII. Plaintiff Dodson stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

284. Plaintiff Dodson received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

285. Upon information and belief, Plaintiff Dodson's PII has not been compromised in a prior Data Breach.

286. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Dodson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: contacting financial institutions to sort out fraudulent activity and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Dodson has spent significant time dealing with the Data Breach, valuable time Plaintiff Dodson otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

287. Plaintiff Dodson suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

288. Plaintiff Dodson further suffered actual injury in the form of experiencing a fraudulent application to open a bank account and debit card at Huntington Bank, in or about September 2023, which, upon information and belief, was caused by the Data Breach.

289. Plaintiff Dodson also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

290. The Data Breach has caused Plaintiff Dodson to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed him of key details about the Data Breach's occurrence.

291. As a result of the Data Breach, Plaintiff Dodson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Dodson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

292. Plaintiff Dodson has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Advance America's possession, is protected and safeguarded from future breaches.

Plaintiff Howard R. Herships

293. Plaintiff Herships was a customer at Advance America, Cash Advance Centers of California, LLC, approximately fourteen years ago.

294. To access the products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

295. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Herships' PII in its system, including his name, Social Security number, and other sensitive information.

296. Plaintiff Herships is very careful about sharing his sensitive PII. Plaintiff Herships stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

297. Plaintiff Herships received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

298. Upon information and belief, Plaintiff Herships' PII has not been compromised in a prior Data Breach.

299. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Herships made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Herships has spent significant time dealing with

the Data Breach, valuable time Plaintiff Herships otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

300. Plaintiff Herships suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

301. The Data Breach has caused Plaintiff Herships to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed his of key details about the Data Breach's occurrence.

302. As a result of the Data Breach, Plaintiff Herships anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Herships is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff John R. Wilkinson III

303. Plaintiff Wilkinson was a customer at Advance America, Cash Advance Centers of Tennessee, Inc.

304. To access the products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

305. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Wilkinson's PII in its system, including his name, Social Security number, and other sensitive information.

306. Plaintiff Wilkinson is very careful about sharing his sensitive PII. Plaintiff Wilkinson stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

307. Plaintiff Wilkinson received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

308. Upon information and belief, Plaintiff Wilkinson's PII has not been compromised in a prior Data Breach.

309. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Wilkinson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Wilkinson has spent significant time dealing with the Data Breach, valuable time Plaintiff Wilkinson otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

310. As a result of the Data Breach, Plaintiff Wilkinson has experienced unknown persons attempting to use his PII. After the Data Breach, Plaintiff Wilkinson received noticed that

he applied for and was denied two credit card applications. Plaintiff Wilkinson never applied for these credit cards.

311. Plaintiff Wilkinson suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

312. The Data Breach has caused Plaintiff Wilkinson to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed his of key details about the Data Breach's occurrence.

313. As a result of the Data Breach, Plaintiff Wilkinson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Wilkinson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Jamila Hunter

314. Plaintiff Hunter was a customer at Advance America, Cash Advance Centers of Florida, LLC.

315. To access the products and/or services at Advance America, she was required to provide her sensitive PII to Advance America.

316. At the time of the Data Breach—on or around February 7, 2023— Advance America retained Plaintiff Hunter's PII in its system, including her name, Social Security number, and other sensitive information.

317. Plaintiff Hunter is very careful about sharing her sensitive PII. Plaintiff Hunter stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

318. Plaintiff Hunter received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

319. Upon information and belief, Plaintiff Hunter's PII has not been compromised in a prior Data Breach.

320. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Hunter made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Hunter has spent significant time dealing with the Data Breach, valuable time Plaintiff Hunter otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

321. Plaintiff Hunter suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

322. The Data Breach has caused Plaintiff Hunter to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed her of key details about the Data Breach's occurrence.

323. As a result of the Data Breach, Plaintiff Hunter anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Hunter is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Eric Speach

324. Plaintiff Speach was a customer at Advance America, Cash Advance Centers of Tennessee, Inc.

325. To access the products and/or services at Advance America, he was required to provide his sensitive PII to Advance America.

326. At the time of the Data Breach—on or around February 7, 2023—Advance America retained Plaintiff Speach's PII in its system, including his name, Social Security number, and other sensitive information.

327. Plaintiff Speach is very careful about sharing his sensitive PII. Plaintiff Speach stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

328. Plaintiff Speach received the Notice Letter, by U.S. mail, directly from Advance America, in August 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

329. Upon information and belief, Plaintiff Speach's PII has not been compromised in a prior Data Breach.

330. As a result of the Data Breach, and at the direction of Advance America's Notice Letter, Plaintiff Speach made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Speach has spent significant time dealing with the Data Breach, valuable time Plaintiff Speach otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

331. After the Data Breach, Plaintiff Speach received the results of a dark web search which confirmed that his PII is available on the dark web.

332. Plaintiff Speach suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly

increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Advance America's possession and is subject to further unauthorized disclosures so long as Advance America fails to undertake appropriate and adequate measures to protect the PII.

333. The Data Breach has caused Plaintiff Speach to suffer fear, anxiety, and stress, which has been compounded by the fact that Advance America has still not fully informed his of key details about the Data Breach's occurrence.

334. As a result of the Data Breach, Plaintiff Speach anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Speach is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

C. Defendants were on Notice of Data Threats in the Industry and of the Inadequacy of their Data Security Systems

335. Defendants were on notice that companies, particularly financial institutions, that maintain large amounts of PII are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information.

336. At all relevant times, Advance America knew, or should have known, that the PII that they collected was a target for malicious actors. Despite such knowledge, Advance America failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' PII from cyber-attacks that Advance America should have anticipated and guarded against.

337. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider*

noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . Many of them were caused by flaws in . . . systems either online or in stores."[4]

338. Additionally, in the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[5]

339. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), Advanced Info Service (8.3 billion records, May 2020), and Morgan Stanley Smith Barney LLC (15 million customers), Advance America knew or should have known that their electronic records would be targeted by cybercriminals.

340. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

341. Additionally, as companies became more dependent on computer systems to run their business,[6] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[7]

---

[4] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[5] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

[6] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[7] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

342. Advance America knew and understood unprotected or exposed PII in the custody of financial institutions, like Advance America, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

343. At all relevant times, Advance America knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Advance America's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

344. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

345. The injuries to Plaintiffs and Class Members were directly and proximately caused by Advance America's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

346. Moreover, PII is a valuable property right.[8] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have

[8] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[9] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

spent over $19 billion on acquiring personal data of consumers in 2018.[10] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

347. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

348. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11]

349. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

[10] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[11] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

D. Cyber Criminals Will Use Plaintiffs' and Class Members' PII to Defraud Them

350. Plaintiffs' and Class Members' PII is of great value to cyber criminals, and the data stolen in the Data Breach has already been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

351. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[12]

352. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[13]

353. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

354. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[14]

[12] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").
[13] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

355. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[15]

356. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[16]

357. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

358. For instance, with a stolen Social Security number, which is only one category of the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[18]

---

[15] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[16] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[17] *Data Breaches Are Frequent*, *supra* note 14.

[18] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

359. Victims of the Data Breach, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[19]

360. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other information for unauthorized activity for years to come.

361. Plaintiffs and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

[19] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

e. Damages flowing from Advance America's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

362. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in the possession of Advance America, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Advance America has shown themselves to be wholly incapable of protecting Plaintiffs' and Class Members' PII.

363. Plaintiffs and Class Members are desperately trying to mitigate the damage that Advance America has caused them but, given the kind of PII Advance America made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII, Plaintiffs and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous

process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[20]

E. Defendants Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' PII

364. Data disclosures and data breaches are preventable.[21] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[22] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[23]

365. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[24]

366. Advance America obtained and stored Plaintiffs' and Class Members' PII—including their Social Security numbers—and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

367. Advance America could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing PII.

---

[20] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[21] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[22] *Id.* at 17.
[23] *Id.* at 28.
[24] *Id.*

368. Advance America did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

369. To prevent and detect cyber-attacks and/or ransomware attacks Advance America could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, customers and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[25]

370. To prevent and detect cyber-attacks or ransomware attacks Advance America could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

[25] *Id.* at 3-4.

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[26]

371. Given that Advance America were storing the PII of its current and former customers, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

F. Value of Personally Identifiable Information

372. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[28]

373. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[26] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.
[27] 17 C.F.R. § 248.201 (2013).
[28] *Id.*

credentials.[29] For example, PII can be sold at a price ranging from $40 to $200.[30] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

374. PII can sell for as much as $363 per record according to the Infosec Institute.[32] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

375. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

376. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

377. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

378. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

[29] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[30] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[31] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.
[32] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

379. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[34] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[35]

380. Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

381. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[36]

---

[33] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf.
[34] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf.
[35] *Id*.
[36] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

382. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[37]

383. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers.

G. Advance America Fails to Comply with FTC Guidelines

384. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

385. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[37] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[38]

386. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[39]

387. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

388. The FTC has brought enforcement actions against lending companies for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

389. These FTC enforcement actions include actions against lending companies, like Advance America.

390. Advance America failed to properly implement basic data security practices.

---

[38] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[39] *Id.*

391. Advance America's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

392. Upon information and belief, Advance America was at all times fully aware of its obligation to protect the PII of its customers. Advance America was also aware of the significant repercussions that would result from its failure to do so.

H. Advance America Fails to Comply with the Gramm-Leach-Bliley Act

393. Advance America is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

394. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

395. Advance America collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Advance America were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

396. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

397. Accordingly, Advance America's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

398. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Advance America violated the Privacy Rule and Regulation P.

399. Upon information and belief, Advance America failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Advance America's network systems.

400. Advance America failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

401. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

402. As alleged herein, Advance America violated the Safeguard Rule.

403. Advance America failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

404. Advance America violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members with a non-affiliated third party without providing Plaintiffs and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

I. Advance America Fails To Comply With Industry Standards

405. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

406. Several best practices have been identified that, at a minimum, should be implemented by lending companies in possession of PII, like Advance America, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Advance America failed to follow these industry best practices, including a failure to implement multi-factor authentication.

407. Other best cybersecurity practices that are standard in the lending industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Advance America failed to follow these cybersecurity best practices, including failure to train staff.

408. Advance America failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

409. These foregoing frameworks are existing and applicable industry standards in the lending industry, and upon information and belief, Advance America failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

J. Common Injuries & Damages

410. As a result of Advance America's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Advance America, and which is subject to further breaches, so long as Advance America fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Victims' Risk Of Identity Theft

411. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

412. As multiple Plaintiffs have already experienced, the unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

413. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

414. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

415. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

416. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[40]

[40] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule

417. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

418. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

419. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

420. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

421. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

---

account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

422. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

423. Thus, due to the actual and imminent risk of identity theft, Advance America encourages Plaintiffs and Class Members to do the following:

> We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. We recommend you review the information contained in the enclosed "Additional Resources" section of this letter. This section describes additional steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.[41]

424. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing freezes and/or otherwise securing their financial accounts; contacting banks to sort out fraudulent activity; signing up for credit monitoring and identity theft insurance; checking if their information was exposed on the dark web; and monitoring their financial accounts for any indication of fraud, which may take years to detect.

425. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

[41] Notice Letter.

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[42]

426. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[43]

427. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[44]

Diminution Value Of PII

428. PII is a valuable property right.[45] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

[42] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[43] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[44] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").
[45] *See, e.g.*, Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

429. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[46]

430. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[47,48]

431. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[49]

432. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[50]

433. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

---

[46] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[47] https://datacoup.com/
[48] https://digi.me/what-is-digime/
[49] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[50] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

434. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, *e.g.*, Social Security numbers.

435. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

436. The fraudulent activity resulting from the Data Breach may not come to light for years.

437. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Advance America's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

438. The injuries to Plaintiffs and Class Members were directly and proximately caused by Advance America's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

439. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, the volume of data obtained in the Data Breach, and multiple Plaintiffs' PII already being disseminated on the dark web (as discussed above), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*,

opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

440. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

441. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[51] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

442. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

443. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Advance America's Data Breach.

Loss Of The Benefit Of The Bargain

444. Furthermore, Advance America's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Advance America and/or its agents for a lending or other services, Plaintiffs and other reasonable consumers understood and expected

[51] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, Advance America did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

CLASS ACTION ALLEGATIONS

445. Plaintiffs bring this action under Federal Rule of Civil Procedure 23 against Advance America, individually and on behalf of all others similarly situated.

446. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**
> All persons residing in the United States whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Nationwide Class" or "Class").

447. In addition, Plaintiffs Rohrer and Garcia propose the following California Subclass definition, subject to amendment as appropriate:

> **California Subclass**
> All persons residing in the state of California whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "California Subclass").

448. Similarly, Plaintiffs Jones and Jennings propose the following Tennessee Subclass definition, subject to amendment as appropriate:

> **Tennessee Subclass**
> All persons residing in the state of Tennessee whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Tennessee Subclass").

449. Similarly, Plaintiffs Lowe, McCreedy, Shilling, Carlisle, and Montalvo propose the following Florida Subclass definition, subject to amendment as appropriate.

Florida Subclass
All persons residing in the state of Florida whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Florida Subclass").

450. Similarly, Plaintiff Lindsey proposes the following Michigan Subclass definition, subject to amendment as appropriate:

Michigan Subclass
All persons residing in the state of Michigan whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Michigan Subclass").

451. Similarly, Plaintiff James proposes the following Indiana Subclass definition, subject to amendment as appropriate:

Indiana Subclass
All persons residing in the state of Indiana whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Indiana Subclass").

452. Similarly, Plaintiff Smelley proposes the following Nevada Subclass definition, subject to amendment as appropriate:

Nevada Subclass
All persons residing in the state of Nevada whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Nevada Subclass").

453. Similarly, Plaintiffs Durham, Dodson, and Turben propose the following Ohio Subclass definition, subject to amendment as appropriate:

Ohio Subclass
All persons residing in the state of Ohio whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Ohio Subclass").

454. Similarly, Plaintiff Kennedy proposes the following Mississippi Subclass definition, subject to amendment as appropriate:

Mississippi Subclass
All persons residing in the state of Mississippi whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Mississippi Subclass").

455. Similarly, Plaintiff Pennington proposes the following Kentucky Subclass definition, subject to amendment as appropriate:

Kentucky Subclass
All persons residing in the state of Kentucky whose personally identifiable information was accessed or acquired as a result of the Data Breach reported by Advance America in August 2023 (the "Kentucky Subclass").

456. Excluded from the Classes are Defendants, any entity in which Defendants has a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

457. Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

458. The proposed Classes meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

459. Numerosity: The proposed Classes are believed to be so numerous that joinder of all members is impracticable. Although the precise number of Class Members is currently unknown to Plaintiff and exclusively in the possession of Defendants, upon information and belief, thousands of individuals were impacted in the Data Breach.

460. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every

other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendants.

461. Adequacy: Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class she seeks to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and their counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

462. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

463. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants failed to adequately safeguard Plaintiffs' and the Class's PII;

c. Whether Defendants' computer systems and data security practices used to protect Plaintiffs' and Class Members' PII violated the FTC Act, and/or state laws and/or Defendants' other duties discussed herein;

d. Whether Defendants owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether they breached this duty;

e. Whether Defendants knew or should have known that their computer and network security systems and business email accounts were vulnerable to a data breach or disclosure;

f. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendants breached contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

h. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate they diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendants' negligent actions or failures to act;

j. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class; and

l. Whether Plaintiffs and Class Members are entitled to treble damages.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of All Plaintiffs and the Nationwide Class against Defendant Purpose Financial, Inc. and on behalf of the state Subclasses as to Defendants Advance America, Cash Advance Centers of California, LLC, Advance America, Cash Advance Centers of Tennessee, Inc., Advance America, Cash Advance Centers of Florida, LLC, Advance America, Cash Advance Centers of Ohio, Inc., Advance America, Cash Advance Centers of Michigan, Inc., Advance America, Cash Advance Centers of Indiana, Inc., Advance America, Cash Advance Centers of Nevada, Inc., Advance America, Cash Advance Centers of Mississippi, LLC., and Advance America, Cash Advance Centers of Kentucky, Inc.)

464. Plaintiffs incorporate by reference the foregoing paragraphs, as if fully set forth herein.

465. All Plaintiffs bring this claim against Defendant Purpose Financial, Inc.

466. Plaintiffs Rohrer, Gibson, and Garcia bring this claim on their own behalf and that of the California Subclass against Defendant Advance America, Cash Advance Centers of California, LLC.

467. Plaintiffs Jones and Jennings bring this claim bring this claim on their own behalf and that of the Tennessee Subclass against Defendant Advance America, Cash Advance Centers of Tennessee, Inc.

468. Plaintiffs Lowe, McCreedy, Shilling, Carlisle, and Montalvo bring this claim on their own behalf and that of the Florida Subclass against Defendant Advance America, Cash Advance Centers of Florida, LLC.

469. Plaintiffs Durham, Dodson, and Turben bring this claim on their own behalf and that of the Ohio Subclass against Defendant Advance America, Cash Advance Centers of Ohio, Inc.

470. Plaintiff Lindsey brings this claim on his own behalf and that of the Michigan Subclass against Defendant Advance America, Cash Advance Centers of Michigan, Inc.

471. Plaintiff James brings this claim on his own behalf and that of the Indiana Subclass against Defendant Advance America, Cash Advance Centers of Indiana, Inc.

472. Plaintiff Smelley brings this claim on his own behalf and that of the Nevada Subclass against Defendant Advance America, Cash Advance Centers of Nevada, Inc.

473. Plaintiff Kennedy brings this claim on his own behalf and that of the Mississippi Subclass against Defendant Advance America, Cash Advance Centers of Mississippi, LLC.

474. Plaintiff Pennington brings this claim on her behalf and that of the Kentucky Subclass against Defendant Advance America, Cash Advance Centers of Kentucky, Inc.

475. Advance America gathered and stored the PII of Plaintiffs and the Class as part of the operation of their business. Defendant Purpose Financial, in concert with its subsidiary companies, jointly implemented a shared network on which the PII of Plaintiffs and Class Members was stored and jointly developed and promulgated the data security policies governing the collection, use, sharing, and retention of Plaintiffs' and Class Members' PII.

476. Upon accepting and storing the PII of Plaintiffs and Class Members, Defendants undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

477. Defendants had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

478. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in Defendants' possession. As such, a special relationship existed between Advance America and Plaintiffs and the Class.

479. Defendants owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their PII, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

480. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

481. Defendants had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendants owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' PII in their possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

482. Only Defendants were in a position to ensure that their systems and protocols were sufficient to protect the PII that had been entrusted to it.

483. Defendants breached their duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendants breached their duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in their possession;

b. Failing to protect the PII in their possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train their employees regarding how to properly and securely transmit and store PII;

d. Failing to adequately train their employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII;

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their PII.

484. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

485. As a proximate and foreseeable result of Defendants' negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

486. Through Defendants' acts and omissions described herein, including but not limited to Defendants' failure to protect the PII of Plaintiffs and Class Members from being stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within Defendants' possession and control.

487. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendants prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII and mitigate damages.

488. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the PII, and closely reviewing and monitoring bank accounts, credit reports, and financial statements.

489. Defendants' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

490. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' negligent conduct.

491. Plaintiffs and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF THE STATE SUBCLASSES AS TO DEFENDANTS ADVANCE AMERICA, CASH ADVANCE CENTERS OF CALIFORNIA, LLC, ADVANCE AMERICA, CASH ADVANCE CENTERS OF TENNESSEE, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF FLORIDA, LLC, ADVANCE AMERICA, CASH ADVANCE CENTERS OF OHIO, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF MICHIGAN, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF INDIANA, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF NEVADA, INC., ADVANCE AMERICA, CASH ADVANCE CENTERS OF MISSISSIPPI, LLC., AND ADVANCE AMERICA, CASH ADVANCE CENTERS OF KENTUCKY, INC.)

492. Plaintiffs incorporate by reference the foregoing paragraphs, as if fully set forth herein.

493. Plaintiffs Rohrer, Gibson, and Garcia bring this claim on their own behalf and that of the California Subclass against Defendant Advance America, Cash Advance Centers of California, LLC.

494. Plaintiffs Jones and Jennings bring this claim bring this claim on their own behalf and that of the Tennessee Subclass against Defendant Advance America, Cash Advance Centers of Tennessee, Inc.

495. Plaintiffs Lowe, McCreedy, Shilling, Carlisle, and Montalvo bring this claim on their own behalf and that of the Florida Subclass against Defendant Advance America, Cash Advance Centers of Florida, LLC.

496. Plaintiffs Durham, Dodson, and Turben bring this claim on their own behalf and that of the Ohio Subclass against Defendant Advance America, Cash Advance Centers of Ohio, Inc.

497. Plaintiff Lindsey brings this claim on his own behalf and that of the Michigan Subclass against Defendant Advance America, Cash Advance Centers of Michigan, Inc.

498. Plaintiff James brings this claim on his own behalf and that of the Indiana Subclass against Defendant Advance America, Cash Advance Centers of Indiana, Inc.

499. Plaintiff Smelley brings this claim on his own behalf and that of the Nevada Subclass against Defendant Advance America, Cash Advance Centers of Nevada, Inc.

500. Plaintiff Kennedy brings this claim on his own behalf and that of the Mississippi Subclass against Defendant Advance America, Cash Advance Centers of Mississippi, LLC.

501. Plaintiff Pennington brings this claim on her behalf and that of the Kentucky Subclass against Defendant Advance America, Cash Advance Centers of Kentucky, Inc.

502. In connection with the dealings Plaintiffs and Class Members had with Advance America, Plaintiffs and Class Members entered into implied contracts with Advance America.

503. Pursuant to these implied contracts, Plaintiffs and Class Members provided Advance America with their PII in order for Advance America to provide lending services to them, and Plaintiffs and Class Members made payments for those services. In exchange, Plaintiffs and Class Members understood that Advance America agreed to, among other things: (1) provide services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' PII; and (3) protect Plaintiffs' and Class Members PII in compliance with federal and state laws and regulations and industry standards.

504. The protection of PII was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Advance America, on the other hand. Indeed, Advance America was clear in its Privacy Policy, and Plaintiffs understood, that Advance America supposedly respects and is committed to protecting customer privacy including by identifying objective security measures.

505. At the time Defendants acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII and not take unjustified risks when storing the PII.

506. Plaintiffs and the Class would not have entrusted their PII to Defendants had they known that Defendants would make the PII internet-accessible, not encrypt sensitive data elements, such as Social Security numbers, and not delete the PII that Defendants no longer had a reasonable need to maintain.

507. Plaintiffs and Class Members performed their obligations under the implied contracts when they provided Advance America with their PII, either directly or indirectly and paid money, including by paying interest, for lending services.

508. Advance America breached its obligations under their implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members' PII in a manner that complies with applicable laws, regulations, and industry standards.

509. Advance America's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class Members have suffered from the Data Breach.

510. Plaintiffs and all other Class Members were damaged by Advance America's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the

confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

511. As a direct and proximate result of Defendants' breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
UNJUST ENRICHMENT
(On Behalf of All Plaintiffs and the Nationwide Class against Defendant Purpose Financial, Inc. and on behalf of the state Subclasses as to Defendants Advance America, Cash Advance Centers of California, LLC, Advance America, Cash Advance Centers of Tennessee, Inc., Advance America, Cash Advance Centers of Florida, LLC, Advance America, Cash Advance Centers of Ohio, Inc., Advance America, Cash Advance Centers of Michigan, Inc., Advance America, Cash Advance Centers of Indiana, Inc., Advance America, Cash Advance Centers of Nevada, Inc., Advance America, Cash Advance Centers of Mississippi, LLC., and Advance America, Cash Advance Centers of Kentucky, Inc.)

512. Plaintiffs incorporate by reference the foregoing paragraphs, as if fully set forth herein.

513. All Plaintiffs bring this claim against Defendant Purpose Financial, Inc.

514. Plaintiffs Rohrer, Gibson, and Garcia bring this claim on their own behalf and that of the California Subclass against Defendant Advance America, Cash Advance Centers of California, LLC.

515. Plaintiffs Jones and Jennings bring this claim bring this claim on their own behalf and that of the Tennessee Subclass against Defendant Advance America, Cash Advance Centers of Tennessee, Inc.

516. Plaintiffs Lowe, McCreedy, Shilling, Carlisle, and Montalvo bring this claim on their own behalf and that of the Florida Subclass against Defendant Advance America, Cash Advance Centers of Florida, LLC.

517. Plaintiffs Durham, Dodson, and Turben bring this claim on their own behalf and that of the Ohio Subclass against Defendant Advance America, Cash Advance Centers of Ohio, Inc.

518. Plaintiff Lindsey brings this claim on his own behalf and that of the Michigan Subclass against Defendant Advance America, Cash Advance Centers of Michigan, Inc.

519. Plaintiff James brings this claim on his own behalf and that of the Indiana Subclass against Defendant Advance America, Cash Advance Centers of Indiana, Inc.

520. Plaintiff Smelley brings this claim on his own behalf and that of the Nevada Subclass against Defendant Advance America, Cash Advance Centers of Nevada, Inc.

521. Plaintiff Kennedy brings this claim on his own behalf and that of the Mississippi Subclass against Defendant Advance America, Cash Advance Centers of Mississippi, LLC.

522. Plaintiff Pennington brings this claim on her behalf and that of the Kentucky Subclass against Defendant Advance America, Cash Advance Centers of Kentucky, Inc.

523. This claim is pleaded in the alternative to the breach of implied contract claim above.

524. Plaintiffs and Class Members conferred a monetary benefit on Defendants, by providing Advance America with their valuable PII without which Defendants could not provide lending services. Plaintiffs and Class Members also paid for Defendants' lending services.

525. Advance America enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

526. Moreover, Advance America retained the PII with no legitimate employment or business purpose.

527. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Advance America instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

528. Under the principles of equity and good conscience, Advance America should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Advance America failed to implement appropriate data management and security measures that are mandated by industry standards.

529. Advance America acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

530. If Plaintiffs and Class Members knew that Advance America had not secured their PII, they would not have agreed to provide their PII to Advance America or would have requested that the PII be deleted upon termination of the employment or business relationship.

531. Plaintiffs and Class Members have no adequate remedy at law.

532. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered the following actual and imminent injuries: (a) monetary harms, including out-of-pocket expenses, loss-of time, and loss of productivity incurred mitigating the present risk and imminent threat of identity theft; (b) actual identity theft and fraud resulting in additional monetary damages; (c) diminution of value of their PII; (d) anxiety, stress, nuisance, and annoyance; (e) increased targeted and fraudulent robocalls and phishing email attempts; (f) the present and continuing risk of identity

theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) the retention of the reasonable value of the PII entrusted to Defendant; and (h) the present and continued risk to PII, which remains on Defendants' vulnerable networks, placing Plaintiffs and Class Members at an ongoing risk of harm.

533. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

534. Advance America should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT IV
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT,
Cal. Civ. Code §§ 1798.100 *et seq*., § 1798.150(a)
(On Behalf of Plaintiffs Garcia and Gibson and the California Subclass against Defendant Advance America, Cash Advance Centers Of California, LLC)

535. Plaintiffs Garcia and Gibson ("Plaintiffs" for purposes of this count) incorporate by reference all allegations of the preceding paragraphs, as though fully set forth herein, and brings this claim solely against Defendant Advance America, Cash Advance Centers of California, LLC ("Defendant" or "Advance America" for the purposes of this count).

536. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

537. Advance America is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of their shareholders or other owners, with gross revenues in excess of $25 million.

538. Plaintiffs and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

539. The personal information of Plaintiffs and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Advance America collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

540. Advance America knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Advance America failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the California Subclass Members. Specifically, Advance America subjected Plaintiffs' and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violations of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

541. As a direct and proximate result of Defendant's violation of their duties, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and California Subclass Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

542. As a direct and proximate result of Defendant's acts, Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiffs' and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

543. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

544. On August 28, 2023, Plaintiff Garcia provided Cash Advance Centers of California, LLC with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Advance America made no response to this notice and Plaintiff is entitled to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

545. On August 30, 2023, Plaintiff Gibson provided Cash Advance Centers of California, LLC with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Advance America made no response to this notice and Plaintiff Gibson is entitled to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

546. Accordingly, Plaintiffs and the California Subclass Members by way of this complaint seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

COUNT V
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code § 17200 *et seq.*
(On Behalf of Plaintiffs Garcia, Gibson, Rohrer, and the California Subclass against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers Of California, LLC)

547. Plaintiffs Garcia, Gibson, and Rohrer ("Plaintiffs" for purposes of this Claim) incorporate by reference all allegations of the preceding paragraphs, as though fully set forth herein, and bring this claim solely against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of California, LLC ("Defendants" or "Advance America" for the purposes of this count).

548. Advance America is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

549. Advance America violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

550. Advance America's "unfair" acts and practices include:

a. failing to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Advance America Data Breach. Advance America failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Advance America's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Advance America's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Advance America's inadequate security,

consumers could not have reasonably avoided the harms that Advance America caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

551. Advance America has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, GLBA, and California common law.

552. Advance America's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' personal information, which was a direct and proximate cause of the Advance America Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Advance America Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Advance America Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and California Subclass Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA.

553. Advance America's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Advance America's data security and ability to protect the confidentiality of consumers' personal information.

554. As a direct and proximate result of Advance America's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

555. Advance America's violations were, and are, willful, deceptive, unfair, and unconscionable.

556. Plaintiffs and California Subclass Members have lost money and property as a result of Advance America's conduct in violation of the UCL, as stated herein and above. Plaintiffs and California Subclass Members paid more than they would have on the belief that Advance America would implement reasonable data security practices and suffered from the lost benefit of their bargain with Defendants.

557. By deceptively storing, collecting, and disclosing their personal information, Advance America have taken money or property from Plaintiffs and California Subclass Members.

558. Advance America acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California Subclass Members' rights.

559. Plaintiffs and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Advance America's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VI
VIOLATIONS OF THE TENNESSEE CONSUMER PROTECTION ACT OF 1977
Tenn. Code Ann. § 47-18-101, *et seq.*,
(On Behalf of Plaintiffs Jones, Jennings, and the Tennessee Subclass against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Tennessee, Inc.)

560. Plaintiffs Jones and Jennings ("Plaintiffs" for purposes of this Claim) incorporate by reference all allegations of the preceding paragraphs, as though fully set forth herein, and bring this claim on behalf of themselves and the Tennessee Subclass solely against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Tennessee, Inc. ("Defendants" or "Advance America" for the purposes of this count).

561. Plaintiffs brings this cause of action pursuant to Federal Rule of Civil Procedure 23, which, procedurally, displaces any state procedural statutory ban on class actions under Tennessee's Consumer Protection Act ("TCPA").

562. Plaintiffs and Tennessee Subclass Members are "natural persons" and "consumers" within the meaning of Tenn. Code § 47-18-103(2).

563. Advance America is engaged in "trade" or "commerce" or "consumer transactions" within the meaning Tenn. Code § 47-18-103(9).

564. The TCPA prohibits "unfair or deceptive acts or practices affecting the conduct of any trade or commerce." Tenn. Code § 47-18- 104.

565. By the acts and conduct alleged herein, Advance America committed unfair or deceptive acts and practices by:

a) failing to maintain adequate computer systems and data security practices to safeguard PII;

b) failing to disclose that their computer systems and data security practices were inadequate to safeguard PII from theft;

c) continued gathering and storage of PII and other personal information after Advance America knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach;

d) making and using false promises, set out in the Privacy Notice, about the privacy and security of PII of Plaintiffs and Tennessee Subclass Members, and;

e) continued gathering and storage of PII and other personal information after Advance America knew or should have known of the Data Breach and before Advance America allegedly remediated the data security incident.

566. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, and Tenn. Code Ann. § 47-18-101, *et seq.*

567. The foregoing deceptive acts and practices were directed at consumers. The foregoing deceptive acts and practices are misleading in a material way because they

fundamentally misrepresent the character of the services provided, specifically as to the safety and security of PII.

568. Advance America's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiffs and members of the Tennessee Subclass, would attach importance to in making their decisions and/or conducting themselves regarding the services received from Advance America.

569. Plaintiffs and Tennessee Subclass Members are consumers who made payments to Advance America for the furnishing of services that were primarily for personal, family, or household purposes.

570. Advance America engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing services to consumers, including Plaintiffs and Tennessee Subclass Members.

571. Advance America engaged in -- and its acts and omissions affect -- trade and commerce, or the furnishing of services in the State of Tennessee.

572. Advance America's acts, practices, and omissions were done in the course of Advance America's business of furnishing consumer services in the State of Tennessee.

573. Moreover, under the Tennessee Identity Theft Deterrence Act of 1999, Defendants were required to accurately notify Plaintiffs and Tennessee Subclass Members if it becomes aware of a breach of its data security systems that is reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Tennessee Subclass Members' Personal Information in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

574. Because Defendants discovered a breach of its security systems in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, Defendants have an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

575. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Tenn. Code Ann. § 47-18-2107(b).

576. As a direct and proximate result of Advance America's multiple, separate violations of the Tennessee CPA and the Tennessee Identity Theft Deterrence Act of 1999, Plaintiffs and the Tennessee Subclass Members suffered damages, as described above.

577. Also as a direct result of Advance America's violations of the Tennessee CPA and the Tennessee Identity Theft Deterrence Act of 1999, Plaintiffs and the Tennessee Subclass Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Advance America to:

a. Ordering that Advance America implement measures that ensure that the PII of its current and former customers is appropriately encrypted and safeguarded when stored on Defendants' network or systems;

b. Ordering that Advance America purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;

c. Ordering that Advance America routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Advance America to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to

third parties, as well as the steps Defendants' current and former customers must take to protect themselves.

578. Plaintiffs bring this action for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Tennessee Subclass Members, and the public from Advance America's unfair, deceptive, and unlawful practices. Advance America's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

579. Advance America knew or should have known that its computer systems and data security practices were inadequate to safeguard Tennessee Subclass Members' PII and that the risk of a data security incident was high.

580. As a result, Plaintiffs and the Tennessee Subclass Members have been damaged in an amount to be proven at trial.

581. On behalf of themselves and other members of the Tennessee Subclass, Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover actual damages, three times actual damages, and reasonable attorneys' fees.

COUNT VII
VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiffs Lowe, McCreedy, Shilling, Carlisle, Montalvo, and the Florida Subclass against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Florida, LLC)

582. Plaintiffs Lowe, McCreedy, Shilling, Carlisle, and Montalvo ("Plaintiffs" for purposes of this Claim) incorporate by reference all allegations of the preceding paragraphs, as though fully set forth herein, and bring this claim on behalf of themselves and the Florida Subclass

solely against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Florida, LLC ("Defendants" or "Advance America" for the purposes of this count).

583. Advance America engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Advance America obtained Plaintiffs' and Florida Subclass Members' PII through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiffs and Florida Subclass Members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

584. As alleged herein this Complaint, Advance America engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failing to implement adequate data security practices to safeguard PII;

b. failing to make only authorized disclosures of current and former customers' PII;

c. failing to disclose that its data security practices were inadequate to safeguard PII from theft; and

d. failing to timely and accurately disclose the Data Breach to Plaintiffs and Florida Subclass Members.

585. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Advance America engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendants' current and former customers.

586. In committing the acts alleged above, Advance America engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or

inadequately disclosing to Defendants' current and former customers that they did not follow industry best practices for the collection, use, and storage of PII.

587. As a direct and proximate result of Defendants' conduct, Plaintiffs and Florida Subclass Members have been harmed and have suffered damages, as detailed above.

588. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and Florida Subclass Members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

589. Also, as a direct result of Defendants' knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Florida Subclass Members are entitled to injunctive relief, including, but not limited to:

a. Ordering that Advance America implement measures that ensure that the PII of its current and former customers is appropriately encrypted and safeguarded when stored on Defendants' network or systems;

b. Ordering that Advance America purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;

c. Ordering that Advance America routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Advance America to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendants' current and former customers must take to protect themselves.

COUNT VIII
VIOLATIONS OF THE MICHIGAN IDENTITY THEFT PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.72, *et seq.*
(On Behalf of Plaintiff Lindsey and the Michigan Subclass against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Michigan, Inc.)

590. Plaintiff Lindsey ("Plaintiff" for purposes of this Claim) incorporates by reference all allegations of the preceding paragraphs, as though fully set forth herein, and brings this claim on behalf of herself and the Michigan Subclass solely against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Michigan, Inc. ("Defendants" or "Advance America" for the purposes of this count).

591. Advance America is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

592. Plaintiff's and Michigan Subclass Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

593. Advance America is required to accurately notify Plaintiffs and Michigan Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

594. Because Advance America discovered a security breach and had notice of a security breach, Advance America had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

595. By failing to disclose the Data Breach in a timely and accurate manner, Advance America violated Mich. Comp. Laws Ann. § 445.72(4).

596. As a direct and proximate result of Defendants' violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass Members suffered damages, as described above.

597. Plaintiff and Michigan Subclass Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT IX
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class against All Defendants)

598. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

599. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 as to all Defendants.

600. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

601. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

602. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

603. Defendants still possess the PII of Plaintiffs and the Class.

604. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial.

605. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Defendants, Plaintiffs and Class Members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

606. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and Class Members, along with other consumers whose PII would be further compromised.

607. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants implement and maintain reasonable security measures, including but not limited to the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering

Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants provide employee training regarding the dangers and risks inherent in using file-sharing websites;

e. Ordering that Defendants cease transmitting PII via file-sharing websites;

f. Ordering that Defendants cease storing PII on file-sharing websites;

g. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for their provision of services;

h. Ordering that Defendants conduct regular database scanning and security checks; and

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

COUNT X
VIOLATIONS OF THE INDIANA DECEPTIVE CONSUMER SALES ACT
Ind. Code § 24-5-0.5
(On Behalf of Plaintiff James and the Indiana Subclass against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Indiana, Inc.)

608. Plaintiff James ("Plaintiff" for purposes of this Claim) incorporates by reference all allegations of the preceding paragraphs, as though fully set forth herein, and brings this claim on

behalf of herself and the Indiana Subclass solely against Defendants Purpose Financial, Inc. and Advance America, Cash Advance Centers of Indiana, Inc. ("Defendants" or "Advance America" for the purposes of this count).

609. The Indiana Deceptive Consumer Sales Act ("IDCSA") "shall be liberally construed and applied to promote its purposes and policies," which include "protect[ing] consumers from suppliers who commit deceptive and unconscionable sales acts." Ind. Code § 24-5-0.5-1.

610. The IDCSA defines a "supplier" as "[a] seller, lessor, assignor, or other person who regularly engages in or solicits consumer transactions, including … a manufacturer, wholesaler, or retailer, whether or not the person deals directly with the consumer." *Id.* § 24-5-0.5-2(a)(3)(A).

611. Defendants are "suppliers" under the IDCSA.

612. The IDCSA defines an "incurable deceptive act" as "a deceptive act done by a supplier as part of a scheme, artifice, or device with intent to defraud or mislead." *Id.* § 24-5-0.5-2(a)(8).

613. The IDCSA regulates the conduct of suppliers, as follows:

> A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.

Id. § 24-5-0.5-3(a).

614. Defendants engaged in incurable deceptive acts under the IDCSA related to consumer transactions with Plaintiff James and Indiana Subclass, as follows:

a. Failing to have appropriate security safeguards or controls in place to prevent exploitation of vulnerabilities within its system that implicated the security of the PII of Plaintiff James and the Indiana Subclass; and

b. Failing to encrypt the sensitive PII of Plaintiff James and the Indiana Subclass, including their Social Security Numbers.

615. The IDCSA provides that "[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater." *Id.* § 24-5-0.5-4(a). Moreover, "[t]he court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (1) three (3) times the actual damages of the consumer suffering the loss; or (2) one thousand dollars ($1,000)." *Id.*

616. The IDCSA provides that a senior consumer, defined as "an individual who is at least sixty (60) years of age," may recover treble damages for an incurable deceptive act. *Id.* §§ 24-5-0.5-2(a)(9), 24-5-0.5-4(i).

617. Plaintiff James and the Indiana Subclass are entitled to and demand recovery of the maximum statutory damages available under the IDCSA.

618. Under IDCSA § 24-5-0.5-4(a), Plaintiff James and the Indiana Subclass are entitled to and demand recovery of reasonable attorney fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendants as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned to represent the Classes as

counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, treble damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Consolidated Class Action Complaint.

Date: November 27, 2023

Respectfully Submitted,

/s/ Dylan A. Bess
DYLAN A. BESS, ESQ. (SC BAR NO. 101648)
MORGAN & MORGAN, ATLANTA PLLC
P.O. Box 57007
Atlanta, GA 30343-1007
Telephone: (404) 965-1886
sbrown@forthepeople.com

Patrick A. Barthle II (pro hac admission pending)
Florida Bar No. 99286
MORGAN & MORGAN

COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 229-4023
Facsimile: (813) 222-4708
pbarthle@ForThePeople.com

Terence R. Coates (pro hac admission pending)
Justin C. Walker (pro hac admission forthcoming)
MARKOVITS, STOCK, & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Interim Class Counsel

Samuel J. Strauss
Raina C. Borrelli
TURKE & STRAUSS LLP
613 Williamson St., Ste. 201
Madison, WI 53703
Phone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

A. Brooke Murphy (pro hac admission forthcoming)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Philip Krzeski (0095713)
CHESTNUT CAMBRONNE PA

100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
pkrzeski@chestnutcambronne.com

William B. Federman (*pro hac vice*)
Interim Co-Lead Class Counsel
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

Plaintiffs' Executive Committee